

# Protéjase del software malicioso

Nos gustaría que Internet fuera un lugar seguro y transparente para todos. Sin embargo, no podemos negar que existen delincuentes y piratas en línea intentando provocar problemas. Una de las maneras de ocasionar problemas es mediante la distribución de software malicioso. Si sabe qué es el software malicioso, cómo se distribuye y cómo evitarlo, puede protegerse.

## ¿Qué es el software malicioso?

El "software malicioso" es un software, de cualquier tipo, diseñado para dañar una computadora. El software malicioso puede robar datos confidenciales de su computadora, disminuir gradualmente la velocidad de su computadora e incluso enviar correos electrónicos falsos desde su cuenta de correo electrónico sin su conocimiento. A continuación, le presentamos algunos tipos de software malicioso habituales que podría conocer:

- **Virus:** Programa informático perjudicial que puede copiarse a sí mismo e infectar a una computadora.
- **Gusano:** Programa informático perjudicial que envía copias de sí mismo a otras computadoras mediante una red.
- **Software espía:** Software malicioso que recopila información de los usuarios sin su conocimiento.
- **Adware:** Software que reproduce, muestra o descarga automáticamente anuncios en una computadora.
- **Troyano:** Programa informático destructivo que aparenta ser una aplicación útil, pero daña su computadora o roba su información una vez que se instala.

## Cómo se distribuye el software malicioso

El software malicioso puede ingresar a su computadora de distintas maneras. A continuación, le presentamos algunos ejemplos comunes:

- si descarga software gratuito de Internet que, de manera oculta, contiene software malicioso;
- si descarga software legítimo que, de manera oculta, se integra con software malicioso;
- si visita un sitio web infectado con software malicioso;
- si hace clic en un mensaje de error falso o en una ventana emergente que inicia la descarga de software malicioso;
- si abre un archivo adjunto de un correo electrónico que contiene software malicioso.

El software malicioso puede distribuirse de diversas maneras, pero eso no significa que no pueda impedirlo. Ahora que ya sabe qué es el software malicioso y lo que puede hacer, veamos algunos pasos prácticos que puede seguir para protegerse.

## Cómo evitar el software malicioso

1. Mantenga su computadora y su software actualizados.

A menudo, Microsoft y Apple lanzan actualizaciones para sus sistemas operativos. Le recomendamos instalarlas cuando estén disponibles para computadoras Windows y Mac. Estas actualizaciones suelen incluir correcciones que pueden mejorar la seguridad de su sistema. Algunos sistemas operativos también ofrecen actualizaciones automáticas, de modo que pueda obtenerlas apenas estén disponibles.

Los usuarios de Windows pueden instalar las actualizaciones mediante una función llamada "Actualización de Windows", mientras que los usuarios de Mac pueden instalarlas con la función "Actualización de software". Si no está familiarizado con estas funciones, le recomendamos que busque más información sobre cómo instalar actualizaciones del sistema en su computadora, en los sitios web de Microsoft y Apple.

Además del sistema operativo, el software de su computadora también debe estar actualizado con las últimas versiones. A menudo, las versiones más nuevas contienen más correcciones de seguridad para evitar ataques de software malicioso.

2. Siempre que sea posible, utilice una cuenta que no sea de administrador.

La mayoría de los sistemas operativos le permiten crear varias cuentas de usuario en su computadora, de modo que distintos usuarios puedan tener diferentes configuraciones. Estas cuentas de usuario también pueden configurarse para que tengan distintas configuraciones de seguridad.

Por ejemplo, una cuenta "admin" (o "de administrador") suele ser apta para instalar software nuevo, mientras que una cuenta "limitada" o "estándar" no suele tener esta característica. Al navegar por Internet diariamente, es probable que no necesite instalar software nuevo. Por lo tanto, le recomendamos que utilice una cuenta de usuario "limitada" o "estándar" cuando sea posible. De este modo, podrá evitar que el software malicioso se instale en su computadora y realice cambios en todo el sistema.

3. Piénselo dos veces antes de hacer clic en vínculos o realizar una descarga.

En el mundo real, probablemente, la mayoría de las personas desconfiaría de entrar a un edificio oscuro con un letrero que dice "Computadoras gratuitas", con luces intermitentes. En la web, debería adoptar un nivel de precaución similar al ingresar a sitios web desconocidos que dicen ofrecer productos gratuitos.

Sabemos que puede ser tentador descargar ese programa gratuito de edición de videos o ese juego de roles, pero, ¿confía realmente en el sitio web que lo ofrece? A veces, es útil salir del sitio web y buscar opiniones o información acerca del sitio web o del programa antes de descargarlo o instalarlo. Una de las principales maneras de recibir software malicioso es a través de las descargas. Por lo tanto, recuerde pensar bien qué está descargando y de dónde lo está descargando.

4. Tenga precaución al abrir archivos adjuntos o imágenes de correos electrónicos.

Si un desconocido le envía una caja de chocolates por correo, ¿la abriría y los comería sin dudarlo? Probablemente, no. De la misma manera, debe tener cuidado si un desconocido le envía un correo electrónico sospechoso con archivos adjuntos o imágenes. A veces, esos correos electrónicos son solo spam. Sin embargo, en otras ocasiones, podrían ocultar software malicioso perjudicial. Si usa Gmail, identifique esos correos electrónicos como spam para que podamos eliminar correos similares en el futuro.

5. No confíe en las ventanas emergentes que le piden que descargue software.

Cuando navega por la Web, es posible que acceda a sitios que muestran ventanas emergentes que lo engañan, ya que le indican que su computadora está infectada y le solicitan que descargue un software para protegerse. No caiga en esta trampa. Cierre la ventana emergente y asegúrese de no hacer clic en ella.

6. Limite el uso compartido de archivos.

Algunos sitios y algunas aplicaciones le permiten compartir fácilmente archivos con otros usuarios. La mayoría de ellos brinda poca protección contra el software malicioso. Si intercambia o descarga archivos mediante el uso compartido, tenga cuidado con el software malicioso. El software malicioso suele estar oculto, aparenta ser una película, un álbum, un juego o un programa popular.

7. Utilice software antivirus.

Si necesita realizar una descarga, le recomendamos que utilice un programa de antivirus para analizarla en busca de software malicioso antes de abrirla. Los software antivirus también le permiten analizar toda su computadora para verificar que no tenga software malicioso. Es una buena idea realizar análisis periódicos de su computadora para encontrar rápidamente software malicioso y evitar que se distribuya. Google no desarrolla software antivirus, pero el artículo siguiente contiene una lista de software antivirus que le recomendamos que tenga en cuenta: [Cómo eliminar software malicioso de su computadora](#).